Protecting Payment Card Data -- A Growing Concern

Douglas A. Dunbar

M&T Bank

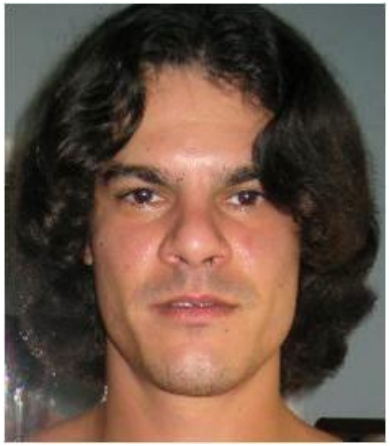
May 12, 2010

M&T Bank

Understanding what's important®

Data Security

Selected media quotes



TJX Hacker Gets 20 Years in Prison - BOSTON — Convicted TJX hacker Albert Gonzalez was sentenced to 20 years in prison on Thursday for leading a gang of cyberthieves who stole more than 90 million credit and debit card numbers from TJX and other retailers - *Wired.com*

….admitted TJX hacker Albert Gonzalez has identified two Russian accomplices who helped him hack into numerous companies and steal more than 130 million credit and debit card numbers. Gonzalez told prosecutors that the hackers breached at least four card processing companies, as well as a series of foreign banks, a brokerage house and several retail store chains - *Wired.com*

"Hacking Ring steals over 40 million credit & debit card numbers"

- *US Department of Justice*

"…breaches reported…indicate criminals continue to target merchants in the hospitality industry, specifically hotels and restaurants." - *VISA Inc.*

M&T Bank

Industry Terms

Alphabet Soup of Data Security….a selected list

- PCI DSS – Payment Card Industry Data Security Standard
- PA DSS – Payment Application Data Security Standard (PABP)
- CVV (CVV2) – Card Verification Value
- Track Data
- PAN – Primary Account Number
- SAQ – Self Assessment Questionnaire
- ASV – Approved Scanning Vendor
- QSA – Qualified Security Assessor
- ROC – Report on Compliance
- QIRA – Qualified Incident Response Analysis
- Acquirer
- Third Party Provider
- CPP – Common Point of Purchase

What data do the bad guys want?

Key cardholder information

- Primary Account Number (PAN)
- Expiration Date
- Cardholder’s Name
- Cardholder’s Address
- Card Security Code (CVV, CVV2, CID)
- PIN / PIN Block
- Track data

Why hackers want the data…

Hacking is a lucrative business

- For personal use in ecommerce setting
  - Often resell purchased merchandise through “eBay” type avenues
- To sell the stolen card data on the internet
  - Price depends on how much data
  - If Track 2 data, they sell to organizations who produce new plastic cards
- To sell the methodology of the exploit
  - Attacker sometimes does this after thorough exploitation of the cards stolen
  - Leads to further exploits on the same merchant by different hackers

NOTE: CPP identification can sometimes lag by months: attacker can hold the cards and not yet use them. The longer the delay, the more difficult it is to find the hacker. The quantity of cards exposed to theft can go up.

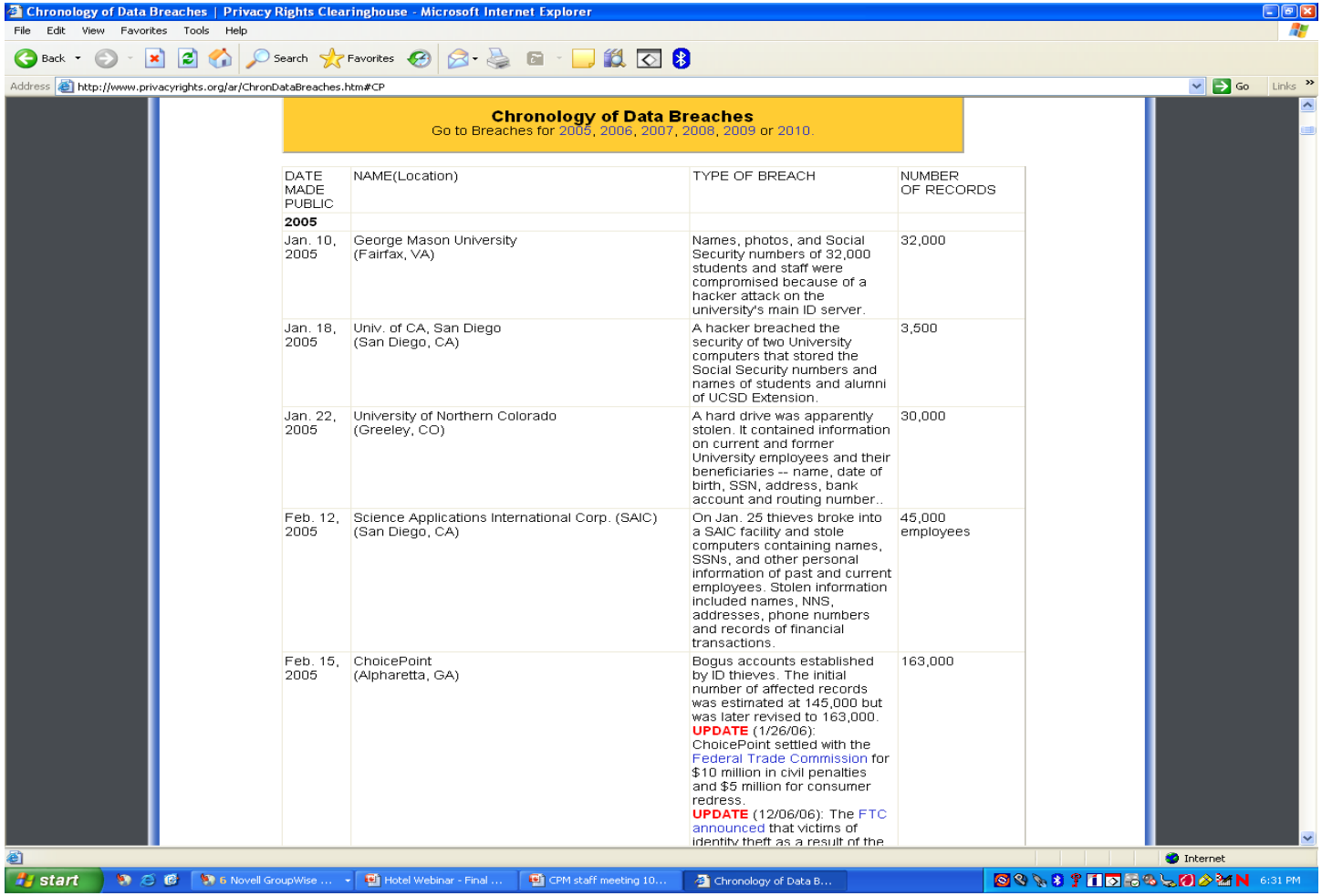
How Hackers Get the Data…

Some common vulnerabilities

- Through “open doors” in the cardholder data network
  - Weak passwords or no passwords
  - Improperly configured remote access or wireless connections to cardholder network
  - Casual internet browsing or email that inadvertently bring malware into the cardholder data environment
- Improper handling of card data in the network environment
  - Deficient payment applications that handle cardholder data improperly
  - Cardholder data was unwittingly stored unencrypted in an unsecured network location
- Through trusted access that should not have been granted
  - Employees have too many privileges
  - Multiple users share login name and password
  - Malicious employees “skim” cards during transaction

How much data has been stolen…

WWW.Privacyrights.org



Chronology of Data Breaches
Go to Breaches for 2005, 2006, 2007, 2008, 2009 or 2010.

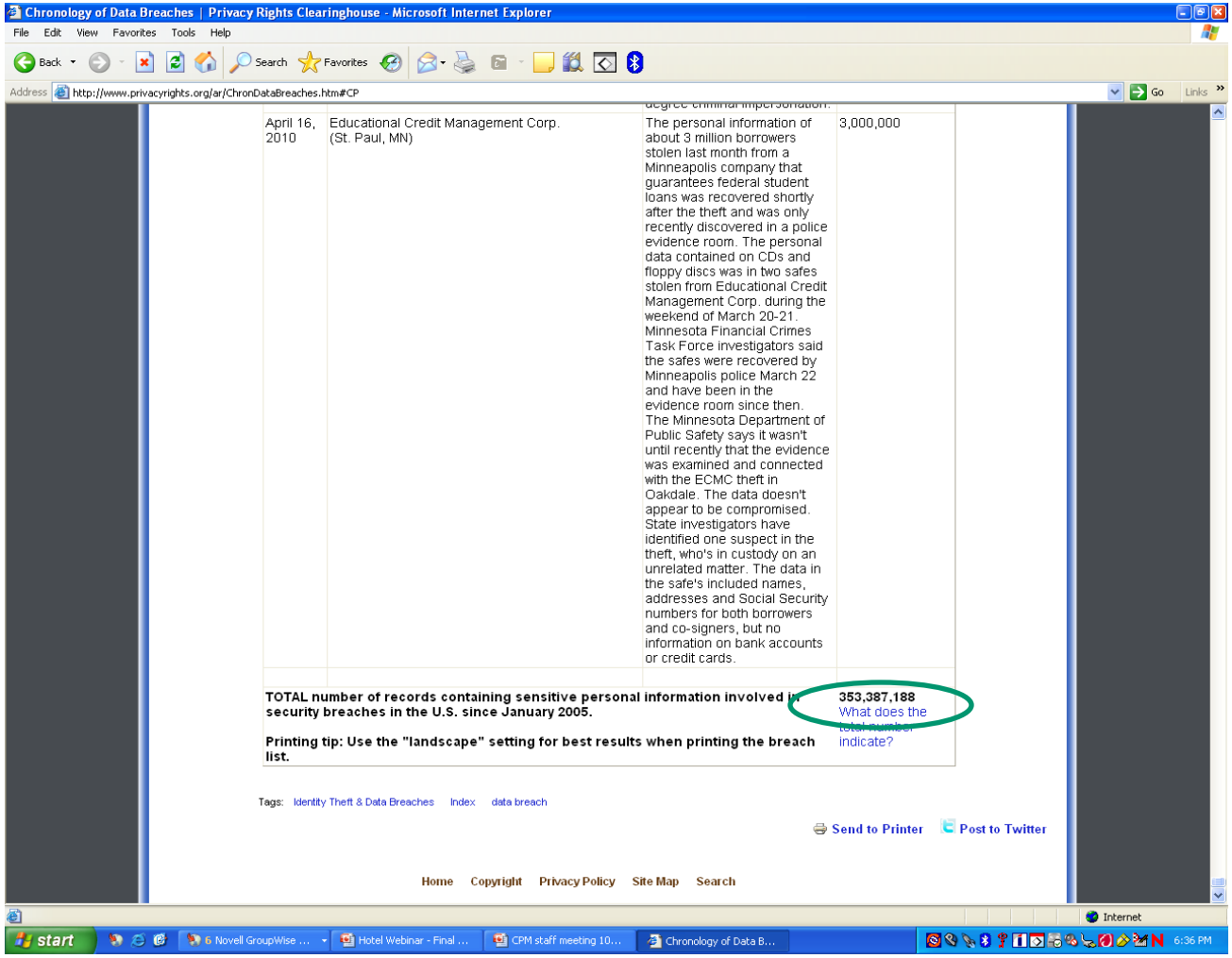
DATE MADE PUBLIC	NAME(Location)	TYPE OF BREACH	NUMBER OF RECORDS
2005			
Jan. 10, 2005	George Mason University (Fairfax, VA)	Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack on the university's main ID server.	32,000
Jan. 18, 2005	Univ. of CA, San Diego (San Diego, CA)	A hacker breached the security of two University computers that stored the Social Security numbers and names of students and alumni of UCSD Extension.	3,500
Jan. 22, 2005	University of Northern Colorado (Greeley, CO)	A hard drive was apparently stolen. It contained information on current and former University employees and their beneficiaries -- name, date of birth, SSN, address, bank account and routing number..	30,000
Feb. 12, 2005	Science Applications International Corp. (SAIC) (San Diego, CA)	On Jan. 25 thieves broke into a SAIC facility and stole computers containing names, SSNs, and other personal information of past and current employees. Stolen information included names, NNS, addresses, phone numbers and records of financial transactions.	45,000 employees
Feb. 15, 2005	ChoicePoint (Alpharetta, GA)	Bogus accounts established by ID thieves. The initial number of affected records was estimated at 145,000 but was later revised to 163,000. **UPDATE** (1/26/06): ChoicePoint settled with the Federal Trade Commission for $10 million in civil penalties and $5 million for consumer redress. **UPDATE** (12/06/06): The FTC announced that victims of identity theft as a result of the	163,000

** Disclaimer: Privacyrights.org reports on publically reported thefts of information, not just those involving card data

M&T Bank

How much data has been stolen…

WWW.Privacyrights.org



With respect to Heartland Payment Systems reported breach:

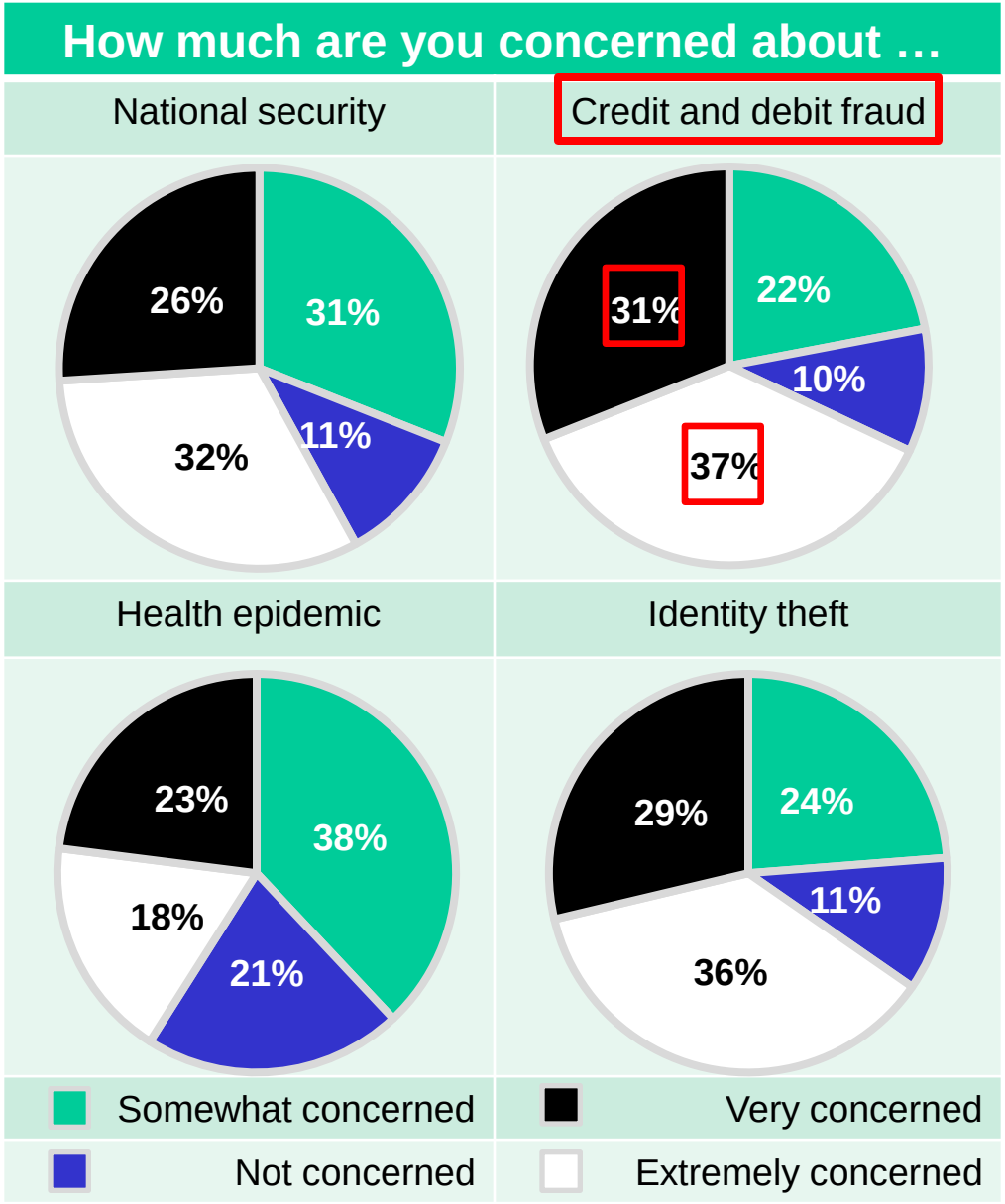
"<u>100 million transactions per month</u> It is unclear how many account numbers have been compromised, and how many are represented by multiple transactions. The number of records breached is an estimate, subject to revision. Consequently, we have not included this breach in the "Total" below."

Privacy Rights Clearinghouse

** Disclaimer: Privacyrights.org reports on publically reported thefts of information, not just those involving card data

M&T Bank

68% of your customers are “very/extremely concerned” about credit card fraud.



Survey conducted in February, 2009 by Unisys Corp

M&T Bank

Protecting your company and customers

…if you store, process or transmit cardholder data

- Become PCI DSS compliant
  - Validation to the standard
  - Level 1-4 merchant
  - SAQ / Scanning / Audit
  - “Ethical Hacking” to identify vulnerabilities
- Remain PCI DSS compliant
  - Compliance is an ongoing responsibility, not an event
- Visa
  - No party that has suffered a data breach involving cardholder data was found to be PCI compliant at the time of the breach
- Think about Third Parties that have access to your data

Data breach
...what is the experience like?

- Catastrophic
  - Consumer notification requirements
  - Loss of customer confidence / Reputational damage
  - Time and energy
  - Forensics process and expense
  - Legal expenses
  - Potential for brands to require audits to PCI DSS as condition for continued card acceptance
  - Fines
  - Fraud / reissuance reimbursement expenses

Ten Keys

Avoiding a Data Compromise

1.	Use POS systems that are fully compliant with PCI DSS. Third-party payment application software must only be selected from the PCI DSS listing of certified applications, PABP (Payment Application Best Practices), or PA-DSS (Payment Application Data Security Standards) • Be certain that the POS system has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's PA-DSS Implementation Guide. (PCI DSS 6.3)
2.	Use "Secure Zones" for storage of cardholder data: additional hardware firewalls should be configured to segregate stored cardholder data away from publicly accessible zones with public-facing IP addresses. (PCI DSS 1.3, 1.3.4) • Implement only one primary function per server. Minimize risk by reducing exposure. (PCI DSS 2.2.1)
3.	Change all default passwords upon installing POS systems. When vendors install POS systems, they often have the default password as "password", or no password at all. "Hardened" passwords must be used and changed on a regular basis. (PCI DSS 2.1) • Establish unique user names and passwords for each individual logging in. (PCI DSS 8.1)
4.	Remote access to the cardholder data environment must be carefully configured, secured and monitored. (PCI DSS 12.3)

M&T Bank

Ten Keys
Avoiding a Data Compromise

5.	Cardholder data should only be displayed in full when absolutely necessary, and any viewing of it must be logged. Otherwise, it should be masked. For example: xxxx1234. (PCI DSS 3.4)
6.	Cardholder data must be encrypted while in transit over public networks. (PCI DSS 4.1)
7.	Make certain that all Anti-Virus software is truly up-to-date on every computer involved with cardholder data network segments. (PCI DSS 5.1)
8.	Ensure all system components and software have the latest vendor-supplied security patches installed (PCI DSS 6.1)
9.	File integrity monitoring software and network intrusion detection systems must be in place which will alert administrators to any unauthorized modifications or access. (PCI DSS 11.4, 11.5) • Track and monitor all access to network resources and cardholder data. Be aware that logging is often not enabled by default, and must be turned on. (PCI DSS 10)
10.	Logs for all system components must be reviewed for malicious activity at least weekly. These logs must be retained for at least one year, with a minimum of three months of online availability. (PCI DSS 10.6, 10.7)

M&T Bank

Data Security
Key takeaways

- Card acceptance is a fact of life in today's economy
  - Hackers are targeting cardholder data in many industries
- Use only PA DSS / PABP applications for Point of Sale
- Have IP addresses scanned for known vulnerabilities
  - "Ethical hacking"
- Become and remain PCI DSS compliant
- Ensure remote access has secure configuration
- Take a hard look at how you answer SAQ questions
- If you do not need the card data, do not store it

Data Security
Resources available

- https://www.pcisecuritystandards.org
- http://visa.com/cisp
- http://www.mastercard.com/us/sdp/merchants/index.html
- https://securitymetrics.com